We can only solve the problem with coordinated action

Moerel, Lokke

Published in:
Magazine BDO Scope

Publication date:
2017

BDO SCOPE

EXPERT UPDATES FOR INTERNATIONAL BUSINESS

'We can only solve the problem with **coordinated action'**

Lokke Moerel Member Dutch Cyber Security Council

CYBERSECURITY: HOW TO MAKE YOURS BETTER

CREATING A RELIABLE **CHAIN**

BDO

‘TWO-FACTOR AUTHENTIFICATION IS A **MUST**’

Digitisation is turning large companies into gold mines for cybercriminals. How can the public and private sectors arm themselves to combat this cyber threat?

Lokke Moerel (51) is Senior of Counsel for international legal firm Morrison & Foerster. Earlier in her career, she worked as ICT Partner for Linklaters and De Brauw Blackstone Westbroek. Moerel is also Professor of Global ICT Law at Tilburg University in the Netherlands and a member of the Dutch Cyber Security Council.

CYBERSECURITY: HOW DO YOU RATE YOURS?

What score does **Lokke Moerel** give to the cybersecurity of Dutch business? 'A 3 (out of 10). Despite the cybersecurity measures taken by individual companies, our networks are so interdependent that, at present, we have few resources with which to counter malicious professional hackers.'

In reality, only a small proportion of all data leaks are caused by hackers and cybercriminals. Most are due to staff errors, such as losing an unencrypted USB stick, leaving a laptop somewhere or running a cloud application that hasn't been approved by their IT department. But here's the good news, says Lokke Moerel: slowly but surely, awareness is growing within organisations 'thanks largely to the Dutch Data Breach Notification requirements, which came into effect early last year'.

Moerel, a lawyer, has worked in the ICT and ICT security sectors for nearly 20 years. She is Senior of Counsel at US law firm Morrison & Foerster, which specialises in technology, and Professor of Global ICT Law at Tilburg University. Moerel was appointed a member of the Dutch Cyber Security Council in 2015.

Has cybercrime really grown so much in recent years or were companies already struggling with it several decades ago?

Moerel: 'Both. Twenty years ago, we had a number of information security cases. One involved a large IT firm losing the credit card details of its clients. They asked us to advise them on whether they should notify the clients concerned. Even then, the answer was "yes", because companies have an obligation to mitigate damages. Neglecting to notify your clients could constitute a tort. In another example, an executive director of a listed company had his briefcase stolen that contained company's interim quarterly results, and the thief could use this knowledge to trade on the stock market (insider trading). The difference between then and now is that these were isolated incidents. Nowadays, cybercriminals are systematically out to hijack confidential company information. The intensity, scale and professionalism of these criminals has grown enormously in recent years.'

'Ensure that you always have adequately encrypted, real-time back-ups'

€15 BILLION WORTH OF **DAMAGE**

The following is a translated extract from the Verhagen report: 'Cybercrime costs the Dutch economy an estimated €15 billion per year, mainly in the form of monetary losses and the misappropriation of valuable intellectual capital. Other attacks involve sabotaging the services and processes of governments and key public infrastructure organisations. This could potentially result in large-scale social disruption – for example, if power plants, transport systems or flood defences are undermined.'

How do you rate the existing cybersecurity awareness of companies?

'It can and should be a lot better. Private companies still aren't sufficiently aware of the dangers of ransomware and cryptoware, which criminals use to encrypt company data that's of no use to them but essential to the company. This data is only released when the company has paid a ransom. Pure extortion, in other words. The data that's "kidnapped" isn't in principle of any interest outside the company and therefore often isn't heavily secured. The solution is simple: ensure you always have securely encrypted, real-time data back-ups so you can always retrieve the data yourself.'

How do the leading Dutch companies score internationally in terms of cybersecurity?

'Most are highly ICT intensive and use centralised ICT systems to which their employees have access, wherever they are at a certain moment in the world. The downside is that because these companies are so highly digitalised, they are automatically more susceptible to cybercrime. Countries where ICT is still more locally organised or where processes are still paper based are less attractive to cybercriminals.'

The Dutch Cyber Security Council recently commissioned PostNL CEO Herna Verhagen to investigate the progress being made with cybersecurity in the Netherlands (see separate story, below left). What do you think of her report?

'It's very good, because it underlines the urgency of the issue for both the government and the private sector. Verhagen concludes that the government needs to take the lead in improving cybersecurity and argues in favour of a national action programme, including an investment agenda. She also recommends the appointment of a National Coordinator, such as we also have for the fight against terrorism. I fully endorse these recommendations, because we won't solve the problem without coordinated action. The Netherlands likes to present itself as a "safe place to do business" but it can't deliver on that promise without adequate cybersecurity.'

Verhagen also stresses companies' duty of care towards their clients.

'Rightly so. Consumers need to be confident they're buying a "cyber-secure" product. The point is a significant one: last autumn, the Dutch Consumer Association brought a civil law action against Samsung, based on its inadequate policy for updating software on Android smartphones. The Consumer Association claimed that Samsung was creating an unsafe situation for consumers because outdated software makes smartphones vulnerable to cybercrime. A ruling hasn't been handed down yet, but this case clearly shows that companies are now expected to adequately secure their products against cybercriminals.' Companies do realise this, but under pressure of 'time-to-market' adequate cybersecurity often suffers. The Dutch Cyber Security Council will shortly issue a guide what the cyber security duties of care are for ICT suppliers.

'Put extra security cordons around data you most want to protect'

Are companies doing enough to improve cybersecurity with their partners in the chain?

Companies that are clearly dependent on other businesses or that work together closely with them more often carry out audits to check the adequacy of their chain partner's cybersecurity. It's in any case logical to do so, especially if you rely on other players to process your employee or customer data or to host your ICT systems. When companies do not have contractual relationships but still work in a chain, there is often still insufficient awareness of their chain dependency.'

The human element, the employee, remains the weakest link in the cybersecurity chain. Are careful training and ongoing refresher courses sufficient?

'They're indispensable, but they're not enough on their own. Securing access to a system using solely password protection isn't sufficient because there'll always be someone who will stick his/her password somewhere or who uses the same password for several systems. "Two-factor authentification" is a must for proper cybersecurity. What's more, simply building a firewall around your internal network and systems is no longer enough to keep cybercriminals at bay. What you should do now is put extra security cordons around the data you most want and need to protect. You should also permanently monitor your own network for any unusual or unexplained data movements that could implicate the presence of an intruder.' ‹